Fortify Scan Issue: Code not scanned

This page has been made public for vendors

Question

What does the Fortify scan issue "Code not scanned" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that code files were delivered that were not included in the Fortify scan. The reviewers cannot determine if this code is production code that wasn't scanned or code that is not part of the production release. Note that the reviewers attempt to ignore code that is obviously test code.

How to detect

Detect this issue by comparing the code to be delivered to the code that was scanned by Fortify. This ensures that all the source code has been scanned and the version that was scanned is the version that is to be deployed. The following steps may be performed to compare the two sets of code:

1. Export the code from the FPR file - this will correspond to the code files that were scanned
    a. Open the FPR in Audit Workbench
    b. Select the Tools -> Extract Source Code menu item
    c. Select the folder to export the code to
2. Compare the extracted code to the source code distribution supplied as part of the secure code review package. You can use WinMerge, diff, or other appropriate application.
    a. Look for **code** files that are in the distribution files that are not in the scanned files. Make sure SQL files, XML configuration files and such are included in the scan. Build files, libraries, images, and other supporting files may be ignored.

How to resolve

For any code files that are delivered, but not scanned perform the following as appropriate:

- Rescan the code and include files that should be in the production build
- Remove files from the delivered code that should not be in the production build
- Include a file with the code review package that indicates why the code files should not be part of the scan (test code, not part of the production build, etc)

References

- **VA Top 10 Fortify Scan Issues For 2017 (Q1)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q4)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q3)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q2)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q1)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q4)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q3)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q2)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q1)**

HPE Fortify Version	4.30 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective -C ☑ Other
Fortify Audit Workbench	☑ Yes ☐ No
Fortify IDE Plugin	☑ Yes ☐ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.